CoVID-19-gerelateerde malware en schadelijke apps

Het is nog niet voldoende dat onze totaal onbekwame Belgische regering ons opzadelde met een corona-nepcrisis en ons nu ook wil opzadelen met speur- en volgsystemen waarmee ze ons recht op privacy schendt en art 17 & 19 van de universele verklaring van de rechten van de mens overtreedt. Dit is een misdadig opzet en de betrokken excellenties staan er niet eens bij stil dat wat zij willen laten doen misdadig is.

In het kielzog van deze bende politieke misdadigers volgen er natuurlijk ook een hele reeks niet-politieke misdadigers. Laat ons maar zeggen dieven, oplichters en bedriegers die garen willen spinnen uit de door de minderheidsregering van lopende zaken bewust geschapen massahysterie, angst en onzekerheid.

Onderzoekers van een wereldbefaamde firma die anti-virussystemen en firewalls verkoopt hebben gevonden dat het aantal CoID-19-gerelateerde schadelijke apps stijgt.

Het staat nu al vast dat 16 corona-virus gerelateerde apps die met ziekte gerelateerde informatie verspreiden en zogezegd gebruikers willen helpen frauduleus zijn bevonden omdat ze gevaarlijke malware verspreiden.

Niet minder dan 30.103 nieuwe corona gerelateerde domeinen werden geregistreerd van dewelke 0,4% (131) kwaadaardig werden bevonden en 9% (2777) verdacht zijn en het voorwerp van nader onderzoek.

Type van Malware.

Deze malware omvat: Mobile Remote Access Trojans (MRATs), Banker Trojans, and Premium Dialers. Dit soort van malware heeft tot doel gevoelige informatie van de gebruikers te stelen

Hidad

Een voorbeeld van deze malware is Hiddad, da afkorting voor “Hidden Ad”. Deze malware bestaat al langer en heeft veel verschillende varianten.Deze keer is er besloten te participeren in de in de coronavirus viering, vermomd als een corona-Informatie app voor Arabisch sprekenden, (wij prijzen ons gelukkig daar niet bij te horen) genoemd رونا ويروس .apk’. Wanneer uitgevoerd verbergt de Hiddad malware zijn icoontje zodat het moeilijk op te sporen is om te verwijderen.

CallPay Premium Dialer

Premium Dialer malware zijn kwaadaardige applicaties voor mobiele toestellen die het slachtoffer abonnee maakt voor te verlenen diensten zonder zijn toestemming en zonder hem te informeren.

MRAT

MRAT staat voor “Mobile Remote Access Trojan”. Het is een type van mobiele malware die toelaat volledige controle over te nemen over mobiele toestellen zoals laptops en gsm’s .

Een MRAT is meestal geïnstalleerd op een toestel om data te stelen of om gebruikt te worden voor localisaties en toezicht. Exact wat onze misdadige regering van plan is of al mee bezig is!

Het is aan te bevelen uw laptop en gsm te beschermen tegen cyberaanvallen met geschikte programma's die zorgen voor veiligheid en kwaadaardige apps opspoort en blokkeert voordat er schade werd aangericht. Laat U nooit software aanpraten door een ondemocratische minderheidsregering van lopende zaken of welke andere overheid ook. Nooit! Overheden zijn nooit te betrouwen. En Belgische al zeker niet!